

TR



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,377	12/20/1999	YURIJ ANDRIJ BARANSKY	Y0999-558	3573

7590 01/03/2007  
ANNE V. DOUGHERTY, ESQ.  
3173 Cedar Road  
Yorktown Heights, NY 10598

EXAMINER
----------

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
----------	--------------

2134

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/03/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

# Office Action Summary

Application No.

09/468,377

Applicant(s)

BARANSKY ET AL.

Examiner

Andrew L. Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 10/4/2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.


## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 December 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
KAMBIZ ZAND  
PRIMARY EXAMINER

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Claims 1-20 are pending.

### ***Response to Arguments***

2. Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new grounds of rejection.

### ***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1, 5, 12-13, and 15-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. With regards to claims 1, 5, 12-13, and 15-16, the cited claims provide the step of "encrypting a second key  $g^b$  using said first key  $b$ " (see step b). Examiner is unclear whether  $g^b$  is being encrypted with  $b$  or if  $g$  is being encrypted by  $b$ . Examiner believes that the claim should read "encrypting a second key  $g$  using said first key  $b$ ."

### ***Claim Rejections - 35 USC § 103***

Art Unit: 2134

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1, 3-4, 7-8, 12, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks" in view of Aziz US Patent No. 5,604,803.

8. With regards to claims 1, 9, 12, 14, 15, and 17, Bellovin teaches randomly generating a first key  $b$  which is known to said content provider and need not be known to said user (Bellovin, Section 3.1, Step 1, A picks a random number  $R_a$ ), the encrypting of a second key using the first key and an encryption algorithm requiring a password (Bellovin, Section 3.1, Step 1, encrypt alpha with  $R_a$  and password), transmitting said encrypted second key  $g^b$  to the client machine (Bellovin, Section 3.1, Step 1, "A sends"), the storing of an encrypted second key on the client machine (Bellovin, Section 3.1, Step 2), decrypting the second key using the first key when the user desires access to data (Bellovin, Section 3.1, Step 2, B also uses shared password  $P$  to decrypt), generating an encryption key  $K_{ab}$  using  $a$  and  $g^b$  (Bellovin, Section 3.1, Step 2, session key is derived), and accessing the data by decrypting an encrypted version of said data at said client machine using the encryption key  $K_{ab}$  (Bellovin, Section 3.1, Step 2, session key). Bellovin lacks a reference to the use of a one-time password. Aziz teaches the use of a one-time password (Aziz, column 6 lines 61-64). At the time the invention was made, it would have been obvious to a person of ordinary skill in the

Art Unit: 2134

art to utilize Aziz's method of using one-time passwords with Bellovin's encryption protocol because it offers the advantage of reducing the likelihood of an unauthorized user gaining access to user passwords (Aziz, column 2 lines 1-13).

9. With regards to claims 3 and 7, Thomlinson as modified teaches the one-time password being a unique user identifier and the one time password being transmitted out of band (Aziz, column 2 lines 45-60).

10. With regards to claims 4 and 8, Thomlinson as modified teaches a second key being required in an algorithm that generates a session key used to decrypt data (Thomlinson, column 10 lines 11-16).

11. Claims 2, 5-6, 10, 13, 16, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin "Encrypted Key Exchange: Password:Based Protocols Secure Against Dictionary Attacks" and Aziz US Patent No. 5,604,803, as applied to claims 1, 12, and 15 above, and in further view of Mi et al US Patent No. 6,418,472.

12. With regards to claims 2, 6, 10, and 20, Bellovin as modified fails to teach the step of transmitting the identity of the client machine to the content provider. Mi teaches the step of transmitting the identity of the client machine to the content provider to authenticate that the user is using the client machine thereby permitted data to be accessed only on the client machine (Mi, column 8 lines 32-46). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Mi's method of transmitting a client's identity with Bellovin as modified because it

Art Unit: 2134

offers the advantage of allowing the identification of a platform or device employed by the user prior to granting access to an object (Mi, column 1 line 69 – column 2 line 2).

13. With regards to claims 5, 13 and 16, Bellovin as modified teaches everything described above and the use of a separate user supplied password (Bellovin, Section 3.1, Steps 1 and 2), but fails to teach the user accessing a web page of said content provider, downloading an applet from said content provider to said client machine. Mi teaches the user accessing a web page of said content provider, downloading an applet from said content provider to said client machine (Mi, column 5 lines 4-21, column 6 lines 15-67). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Mi's applet procedure with Bellovin as modified because it offers the advantage of providing a tamper resistant user friendly method of authentication that helps identity a user (Mi, column 1 line 61 – column 2 line 5).

14. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin "Encrypted Key Exchange: Password:Based Protocols Secure Against Dictionary Attacks," Aziz US Patent No. 5,604,803, and Mi et al US Patent No. 6,418,472, as applied to claims 2 and 6 above, and in further view of Thomlinson et al US Patent No. 6,389.

15. With regards to claims 18-20, Bellovin as modified teaches authenticating the user to said content provider based on said stored mapping (Mi, column 4 lines 45-52, column 5 lines 43-60). Bellovin as modified fails to teach generating a new encryption

Art Unit: 2134

key based on said second key, encrypting a new encryption key based on said second key, encrypting said additional data with said new encryption, and transmitting said encrypted additional data to said client machine whereat the new encryption key is decrypted using said second key and said encrypted additional data is decrypted using said new encryption key. However, Thomlinson teaches generating a new encryption key based on said second key (Thomlinson, column 9 lines 20-22, master key), encrypting a new encryption key based on said second key (Thomlinson, column 9 lines 20-22, item key encrypted by master key), encrypting said additional data with said new encryption key (Thomlinson, column 9 lines 13-19), and transmitting said encrypted additional data to said client machine whereat the new encryption key is decrypted using said second key and said encrypted additional data is decrypted using said new encryption key (Thomlinson, column 10 lines 15-16). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify Bellovin as modified with Thomlinson because it offers the advantage of protecting sensitive transactions from unauthorized access (Thomlinson, column 1 lines 40-45).

16. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable Thomlinson et al US Patent No. 6,389,535 and Aziz US Patent No. 5,604,803, as applied to claim 9 above, and further in view of Schneier Applied Cryptography.

17. With regards to claim 11, Bellovin as modified, lacks a reference to a MAC authentication procedure. Schneier describes the one-way hash function termed a MAC that is used to verify authenticity (Page 455, Section 18.14). At the time the

Art Unit: 2134

invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's MAC authentication on  $g^{a^b}$  to authenticate the server to the client because it provides a verification method that is reliant on having the same key. Both client and server generate the same key during the authentication procedure so the MAC authentication would be an easy way to check authenticity without needing security since it is a one-way function (Page 455, Section 18.14).

### ***Conclusion***

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.



If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571 272 3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.



Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven



KAMBIZ ZAND  
PRIMARY EXAMINER